Жамият ва инновациялар –
Общество и инновации –
Society and innovations
Journal home page:
https://inscience.uz/index.php/socinov/index

Legal framework for privacy in technological advanced society

Bekhzod Muminov [1]

High School Judges With the supreme judicial council of the Republic of Uzbekistan

ARTICLE INFO

Article history:
Received September 2020
Received in revised form
15 September 2020
Accepted 15 October 2020
Available online
30 October 2020

Keywords:
privacy
search
seizure
conversation
communications
probable cause
personal data
reasonable expectation
reasonableness, electronic mail
third party doctrine.

ABSTRACT

This article will review the genesis of the "reasonable expectation of privacy" ("REP") requirement, both to establish the governing legal framework and to demonstrate how changing technology has altered our conception of the privacy in the past and describes the limits and ability of government agents to search for and seize evidence without a warrant

Технологик ривожланган жамиятда шахсий хаёт дахлсизлигининг ҳуқуқий асослари

Калит сўзлар:
шахсий ҳаёт
тинтув
олиб қўйиш
сўзлашув
коммуникация
етарли асос
шахсий маълумотлар
асосли ишонч
асослилик
электрон почта
учинчи тараф доктринаси.

АННОТАЦИЯ

Мазкур мақолада “шахсий ҳаёт дахлсизлигига ишонч” ("REP") тушунчасининг генезиси, зарур ҳуқуқий асосларини аниқлаш ва ўтмишдаги шахсий ҳаёт дахлсизлиги концепциясининг қандай ўзгарганлиги таҳлил қилиниб, мансабдор шахсларнинг далилларни санкциясиз излаш ва олиб қўйиш юзасидан чегаралари ва имкониятлари баён қилинган.

[1] PhD, assistant professor, High School Judges With the supreme judicial council of the Republic of Uzbekistan, Tashkent, Uzbekistan
E-mail: b.muminov123@gmail.com

Правовые основы неприкосновенности личной жизни в технологически продвинутом обществе

Ключевые слова:
личная жизнь
поиск
изъятия
переговоры
комуникации
разумная причина
личные данные
оправданное ожидания
обоснованность
разумные ожидания
разумность
электронная почта
доктрина третьей стороны.

АННОТАЦИЯ

В статье рассматриваются генезис понятия «оправданный расчёт на неприкосновенность личной жизни»(«REP»), чтобы установить регулирующую правовую основу и продемонстрировать, как меняющиеся технологии изменили нашу концепцию неприкосновенности личной жизни в прошлом и описывает пределы и возможности должностных лиц по поиску и изъятию доказательства без получения санкций.

INTRODUCTION

As stated in the OSCE Copenhagen Document 1990, “the rule of law does not mean merely a formal legality which assures regularity and consistency in the achievement and enforcement of democratic order, but justice based on the recognition and full acceptance of the supreme value of the human personality and guaranteed by institutions providing a framework for its fullest expression”.[2]

On July 2, 2019, the Republic of Uzbekistan adopted the first special law that regulates the protection of personal data. The Law, which comes into force on October 1, 2019, provides a variety of legal obligations for government agencies.

The main characteristic behalf criminal cases is that they are brought in the name of the government on behalf of the community. But while the presence of the state as a party is a feature of criminal cases, it is also a feature of many civil cases and of administrative proceedings brought by government agencies which are generally thought to be civil.

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks declares article 12 of Universal Declaration of Human Rights[3]

When government focuses its attention on crime detection and crime prevention, frequently it encounters uncooperative individuals. But the police are not compelled to forego investigative and preventive measures for lack of voluntary cooperation. They can exert themselves in order to gather information, evidence and suspects. When they do they must consider limitations imposed by the Constitution and Code of Criminal Procedure. Implicit in this thesis to deprive any person of life liberty or property without due process of law in itself unconstitutional.

[2] OSCE Copenhagen Document, 29 June 1990, Part 1 par 94. http://www.osce.org/fr/odihr/elections/14304>.
[3] https://www.un.org/en/universal-declaration-human-rights/

LEGAL GROUNDS FOR PRIVACY.

According to the Code of Criminal Procedure privacy of correspondence, telegraph messages and telephone conversations shall be protected by law. Search, seizure, view of home or other premises and territories, belong to a person, arrest of the postal and telegraph correspondence and its seizure from the postal offices, tapping of telephones and of the other communication equipment, can be carried out only and in accordance with the procedure established by the Code. Tapping of telephone conversations, familiarization with communications, obtaining data about them, as well as other limitation of secrecy of conversations and communications is allowed only in cases and order, stipulated by law. For example, law enforcement bodies of Uzbekistan may obtain access to such conversations and communications during investigation of a crime[4].

The general rule is that right of the people mentioned above shall not be violated and no warrants shall issue but upon probable cause.

These considerations do not vanish when the search in question is transferred from the setting of a home, an office, or a hotel room to that of a virtual world. Where ever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures. However courts had difficulty applying

privacy regulations to modern investigative techniques.

According to Article 7 of the Law, the Cabinet of Ministers of the Republic of Uzbekistan is in charge of the regulation of personal data. The personal data can be processed after obtaining the consent of subjects. The consent can be expressed in any form that allows verifying its existence. The subject may withdraw their consent at any time. The operator should define the purposes of data processing[5].

Personal information was further elucidated in Freedom of Information Law which determines personal information about citizens as confidential. It is prohibited to collect, keep, process, disseminate and use information about private life, as well as information that violates secrecy of private life, secrecy of correspondence, telephone conversations, mail, telegraph and other information of the citizen without obtaining his consent. Above mentioned information might be provided only in exceptional cases to the entities, who are entitled to use such data as per Uzbek laws, such as law enforcement bodies, courts, tax and statistical bodies[6].

However, those who commit crimes have not missed the information revolution. Criminals use electronic devises and network in the course of committing their crimes. For example, the net can be used to deliver a death threat by mail, for hacker attacks against a vulnerable computer network, to disseminate computer viruses, or to transmit images of child pornography. In other cases, computers merely function as convenient storage devices for evidence of crime.

Has the reasonable expectation of privacy test become outmoded in our technological advanced society where little of any information can be kept private ? Has the electronic devise user legitimate expectation of privacy within the web addresses that he visits or the e-mail addresses to which he sends e-mail, as this information is accessible to his internet service provider ?.

[4] **Criminal Procedure Code of the Republic Of Uzbekistan**
[5] https://lex.uz/
[6] https://lex.uz/

REASONABLENESS AS PREDOMINANT CLAUSE

Considering only whether a search is reasonable under the circumstances, as a unanimous Supreme Court stated in 2001,the touchstone of the Fourth Amendment is reasonableness, and the reasonableness of a search is determined "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate government interests[7].

Reasonableness requires a court to compare the intrusion upon privacy with the government need. One element of government need could be termed "fungibility." If the same information is available via other less intrusive means, the greater intrusion is likely to be unreasonable. Thus, the fact that a low-cost, technologically enhanced search can obtain needed information should not itself be sufficient to render that search constitutional. Another logical element of government need is the magnitude of the crime at issue.

Technology will permit searches that may seem less intrusive but that obtain the same quantum of information-perhaps a scan by a passive millimeter wave camera rather than a full-body pat-down, or a single search of an extensive database rather than a significant background investigation. Including the magnitude of the alleged crime in the analysis may prevent courts from too freely authorizing intrusive conduct[8].

Professor Henderson argues that the reasonable expectation of privacy test should be dropped in favor of a test that evaluates every government invasion by whether it is reasonable under the circumstances in other words “technology will lead to no privacy and police practice will incorporate that technology to create a reality of no privacy[9].

According to Professor Grey courts constitutionally apply policy considerations not articulated in the text of the Constitution in the course of judicial review and the courts have a role as the expounder of basic national ideals of individual liberty and fair treatment, even when the content of these ideals is not expressly attributable to the Constitution[10].

The dramatic increase in computer-related crime requires investigators to understand how to obtain electronic evidence stored in electronic devices.

Grounds for searching implicit from Code of Criminal Procedure states that the investigator, inquiry officer may search if have sufficient information to believe that some living, office, production premises or any other site contain or any person has items and documents important for the case quite vague. It has been argued that the main remedy for an unconstitutional search and seizures is exclusion.

Thus reasonableness clause is the predominant clause most notably when the governments search or seizure serves special needs beyond criminal law enforcement. The term “probable cause” is used to define the minimum showing necessary to support a warrant application; it is not used to demarcate reasonableness generally in search and seizure situations. But despite the placement of the words, the decisions make probable cause a limitation on many searches and seizures seizure even though no warrant is deemed necessary under the circumstances. The fact that the definition of probable cause is not clear means that prosecutor and court have been left to give meaning to the term.

---

[7] United States v. Knights, 534 U.S. 112, 118-19 (2001).
[8] United States v. Torres, 751 F.2d 875, 882 (7th Cir. 1984)
[9] Henderson (2005) Nothing new under the sun: A Tecnologically Rational Doctrine of Fourt Amendment Search. Mercer Law Review Vol. 56, No. 507, 2005
[10] See Grey, .Do We Have An Unwrillen Constitution?, 27 STAN. L. REV. 703 (1975).

Initially, supporters of this point of view contend that surveillance technique involved no physical penetration is nor subject of protection. What an individual knowingly exposes to the public even in his own home or office **can't be** protected. But gradually this view had to change significantly.

For instance in Olmstead v. United States the Court stated, "The amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only."[11]

Thus in 1928 when the Supreme Court of US first encountered the relatively novel technology of telephone wiretapping, it held the practice did not constitute a Fourth Amendment search. At that time approximately forty-one percent of U.S. households were equipped with telephone service."[12]

But by 1967, when eighty-seven percent of households were so equipped[13], the Court, influenced by the increasing prevalence and importance of the telephone in society, reversed course: person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication[14].

It is undeniable that changing technology has altered our conception of privacy. Electronic mail has rapidly become a familiar form of communication, despite its potential insecurities. There are over 3.9 billion **email users worldwide**. In 2018, **email users** had an average of 1.75 **email** accounts. Over 293 billion **emails** are sent each day throughout the world[15]. There are 1.3 billion Messenger users globally. More than 20 billion messages are exchanged between business and users monthly on Facebook Messenger[16].

Technology now enables voluminous important messages and confidential conversations to occur through an enormous system of electronic networks. These advances, however, raise significant privacy concerns. We are placed within the uncomfortable position of not knowing who might access to our personal and business e-mails, our medical and financial records, or our cordless and mobile phone conversations .

The Uzbekistan criminal procedure code provides for search and seizure of post and telegraph communications and wiretapping of telephone or other communications of persons under criminal investigation upon authorisation by the prosecutor or a court (Articles 166-170).[17]

Take all necessary measures to ensure that communications surveillance and collection of personal data in Uzbekistan conform to its obligations under the International Covenant on Civil and Political Rights, including article 17; in particular, measures should

[11] 277 U.S. 438 (1928)
[12] U.S. Census Bureau, Statistical Abstract of the United States: 2003, No. HS-42, Selected Communications Media: 1920 to 2001, at http://www.census.gov/statab/histlHS42.pdf.
[13] Webb & Assoc., Telecommunications History Timeline: The 1920s, at www.webbconsult.com/1920.html.
[14] Katz, 389 U.S. at 352.
[15] https://99firms.com/blog/how-many-email-users-are-there/#gref
[16] https://review42.com/facebook-messenger-statistics/
[17] Criminal Procedure Code of the Republic Of Uzbekistan

be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity[18].

THIRD PARTY DOCTRINE

According to this doctrine, one retains no reasonable expectation of privacy in information provided to a third party and it is susceptible to creating these kind of arbitrary distinctions command is that any search or seizure be reasonable. That is to say, if someone has voluntarily given his message to any number of persons, and consequently have no reasonable expectation of privacy. On the opposite hand what he seeks to keep as private, even if accessible to the open view, may be constitutionally protected.

When investigators learn of data possessed by third parties that may provide evidence of a crime, they may wish to examine it. Whether the law requires a warrant before examining the information depends on if the third-party possession has eliminated the individual's reasonable expectation of privacy.

Doubtless, doctrine is crucial for doctrinal clarification, namely whether there is a reasonable expectation of privacy in electronic mail in unencrypted and encrypted form.

If information is considered as confidential and its disclosure may cause harm to the rights and interests of individual provision of such information to third parties can be rejected. The owner or holder of confidential information should inform the agency that requests confidential information about limitation to such information.

Under Telecommunications Law nobody is allowed to break secrecy of telephone conversations, telegraph and other correspondence, transmitted through telecommunication networks. All operators and providers shall ensure secrecy of such conversations and communications[19].

If courts were to find no REP in the contents of e-mail because it is necessarily conveyed to others, they would either have to find likewise for the contents of modern telephone conversations, an unlikely result, or create an anomaly whereby digitized voice content passing through precisely the same systems retains a REP that e-mail content does not[20].

"Knowing exposure" should not remove information from the protection of the Constitution, but rather only affirmative desire that content be utilized by a third party.

On the other hand the third party doctrine is objectionable even if limited as recommended because, it treats privacy as an indivisible commodity-once information is given to any one party for any one purpose.

However, when encryption's ability to guarantee confidentiality applied making the message unintelligible to anyone other than intended recipient it is clear that sender intended to guarantee privacy one and retained a reasonable expectation of privacy.

Expectation of privacy would be determined by operating laws and practices. To determine whether an individual has a reasonable expectation of privacy in information stored in an electronic devise, it helps to treat the devise like a closed container. Generally law prohibits law enforcement from accessing and viewing information stored in a devise if it would be prohibited from opening a closed container and examining its contents in the same situation. For instance, do individuals have a reasonable expectation of privacy in the

[18] https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf
[19] https://lex.uz/
[20] Cleared for Take-off ? Mobile Phones on Planes, ECONOMIST, Apr. 3, 2004 (available at 2004 WL 62017484)

contents of their electronic devices ? If the answer is “yes,” then the investigator ordinarily must obtain a warrant, or fall within an exception to the warrant requirement, before it accesses the information stored inside. As a result, accessing information stored in a computer in a normal way will implicate the owner’s reasonable expectation of privacy.

This is in line with rule established in Article 19 of Code of Criminal Procedure which states that the Private postal correspondence and private phone messages can be disclosed during the open court hearing only upon the consent of persons, who has sent and received these letters and messages. Otherwise they shall be disclosed and studied in the closed court hearing[21].

Genesis of the "reasonable expectation of privacy" ("REP") requirement, both to establish the governing legal framework and to demonstrate how changing technology has altered our conception of the privacy in the past.

Effect the purpose of the framers of the Constitution in the interest of liberty ... cannot justify enlargement of the language employed beyond the possible practical meaning of houses, persons, papers, and effects, or so to apply the words search and seizure as to forbid hearing or sight."[22]

Another important aspect is exceptions to the warrant requirement in cases involving electronic data. Investigator wishing to justify such an intrusion must proffer an adequate rationale, such as exigent circumstances. The exigent circumstances exception to the warrant requirement generally applies when one of the following circumstances is present: evidence is in imminent danger of destruction, “hot pursuit” of a suspect, the suspect is likely to flee before the officer can get search warrant. In determining whether exigent circumstances exist, should be considered: the degree of urgency involved, the amount of time necessary to obtain a warrant, the evidence may be removed or destroyed, the possibility of danger at the site. Exigent circumstances can arise in electronic data cases prior to the evidence has been secured because electronic data is not stable as material evidence. Electronic data can be put out of law enforcement reach with encryption programs with just a few keystrokes.

RECOMMENDATION

When investigating cases involving electronic data to what extent established exceptions are applicable to new technologies should be reconsidered one more time.

1. Consent which means that investigators may search object without a warrant if a person with authority has voluntarily consented to the search.

2. Implied Consent when individuals often enter into agreements with the government in which they waive some of their constitutional rights. For example, bank clerks may agree to be searched as a condition of employment, and visitors to buildings may agree to a search of their person and property as a condition of entrance. In a similar way, computer users may waive their rights to privacy as a condition of using the systems.

3. After the lawful arrest, agents may conduct a full search of the arrested person, and a more limited search of his surrounding area, without a warrant.

4. In order to protect the government’s ability to monitor contraband and other property that may enter or exit illegally, the Code has recognized a special exception to the warrant requirement for searches that occur at the border. According to the law,

[21] https://lex.uz/
[22] Olmstead, 277 U.S. at 465

routine searches at the border do not require a warrant, probable cause, or even reasonable suspicion that the search may uncover contraband or evidence.

5. Whereas private-sector employees enjoy a reasonable expectation of privacy, government employees retain a reasonable expectation of privacy with in the workplace on condition that case-by-case inquiry shows that it is reasonable for employees to expect privacy. Whether a specific policy eliminates a reasonable expectation of privacy could be a factual question.

Employment policies of many employers stated that the supervisors would inspect, and/or monitor Internet access and that such auditing would be implemented to support identification and prosecution of unauthorized activity.

In a common computer case, investigators learn of online criminal conduct. Using records obtained from a victim or from a service provider, investigators determine the Internet Protocol address used to commit the crime. Then investigators compel the Internet Service Provider to identify which of its customers was assigned that IP address at the relevant time, and to provide the user's name, street address, and other identifying information. In some cases, investigators confirm that the person named by the ISP permanent address. Such affidavits often sufficient to set up probable cause. However sometimes defendants may argue that the association of an IP address with address is insufficient to set up probable cause because it is possible for individuals not residing at that address and using Internet connection.

The programmatic purpose of a search may determine its constitutionality, meaning that for searches not based upon individualized suspicion and probable cause, the constitutionality of the search may depend upon its purpose."[23]

As Harold Krent has argued, "the reasonableness of a seizure extends to the uses that law enforcement authorities make of property and information."[24]

Thus, if police wish to conduct a technologically-enhanced search, the proposed uses of information so obtained should factor into the reasonableness inquiry.

While our privacy is surely invaded by government agents scanning persons or homes to prevent a terrorist attack or to protect a passing dignitary, it nonetheless might be more reasonable if they agree not to share that information with those pursuing ordinary law enforcement ends.

Unless external restraint, technology will lead to an expectation of no privacy, and police practice will incorporate that technology to create a reality of no privacy. Although legislation is always welcome in this area, and is crucial when it comes to protecting our privacy.

Coherent regulation of any power requires an integration of the terms in which the power is authorized and the terms by which it is limited; and an agency which controls some of the terms of limitation but none of the terms of authorization is generally likely to prefer mobility to consistency in its regulatory techniques. However, the degree to which mobility must be maintained and consistency must be sacrificed to maintain it depends upon the extent of variability that can be expected in the practices that the Court is called upon to regulate[25].

[23] See Edmond, 531 U.S. at 45-46 "Programmatic purposes may be relevant to the validity of Fourth Amendment intrusions undertaken pursuant to a general scheme without individualized suspicion.
[24] Harold J. Krent, Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment, 74 TEX. L. REV. 49, 51 (1995).
[25] Amsterdam, Perspectives on the Fourth amendment, 58 Minn.L.Rev. 384(1974)

It is true, as Mr. Justice Holmes said, that "[w]henever the law draws a line there will be cases very near each other on opposite sides.[26]

On the one hand where guilt is not certain before the intrusion the police may be invading legitimate privacy and possessory interests of those who are actually innocent.

CONCLUSION

Accordingly, investigators must consider two questons when **requesting** for computer search and seizure warrant. First, does the search violate a reasonable expectation of privacy and whether the search permissible within an exception to the warrant requirement? The privacy interest invaded must be one that society is prepared to accept as reasonable or legitimate.

Expectation of privacy would be determined by existing laws and practices and search must also be both “justified at its inception” and “permissible in its scope. Limited third party doctrine, requires police to avert their "technologically-enhanced" eyes from information otherwise provided. Programmatic purpose of a search may determine its constitutionality, meaning that for searches not based upon individualized suspicion and probable cause, the constitutionality of the search may depend upon its purpose. Accordingly, REP test and a limited third party doctrine provide protection for many technologically-enhanced searches. Considered our prospects for developing any generally effective control over police practices third party doctrine should be adopted to the intrusive capability of modern technology.

Sometimes criminal procedure presents a tension: the necessity to guard individual defendants and promote individual freedom is pitted against state interests in prosecuting crime and maintaining security. Expansion of judicial control over the inquiry and preliminary investigation within the framework of further expansion of the institution of "Habeas Corpus" based on best practices of foreign countries must become an effective means of ensuring protection of citizens' rights and freedoms from criminal encroachments, as well as avoiding violations of their legitimate interests.

The court has the final say in interpreting constitutional protections concerning privacy in criminal procedure, enhanced protection of constitutional rights through constitutional reliance, can provide greater protections of rights.

REFERENCES

1. OSCE Copenhagen Document, 29 June 1990, Part 1 par 94. http://www.osce.org/fr/odihr/elections/14304>.

2. https://www.un.org/en/universal-declaration-human-rights/

3. Criminal Procedure Code of the Republic Of Uzbekistan

4. United States v. Knights, 534 U.S. 112, 118-19 (2001).

5. United States v. Torres, 751 F.2d 875, 882 (7th Cir. 1984)

6. Henderson (2005) Nothing new under the sun: A Tecnologically Rational Doctrine of Fourt Amendment Search. Mercer Law Review Vol. 56, No. 507, 2005

7. Grey, Do We Have An Unwrillen Constitution?, 27 STAN. L. REV. 703 (1975).

[26] United States v. Wurzbach, 280 U.S. 396, 399 (1930)

8. U.S. Census Bureau, Statistical Abstract of the United States: 2003, No. HS-42, Selected Communications Media: 1920 to 2001, at http://www.census.gov/statab/histlHS42.pdf.

9. Webb & Assoc., Telecommunications History Timeline: The 1920s, at www.webbconsult.com/1920.html.

10. Katz, 389 U.S. at 352.

11. https://99firms.com/blog/how-many-email-users-are-there/#gref

12. https://review42.com/facebook-messenger-statistics/

13. https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf

14. Cleared for Take-off ? Mobile Phones on Planes, ECONOMIST, Apr. 3, 2004 (available at 2004 WL 62017484)

15. Olmstead, 277 U.S. at 465

16. Amsterdam, Perspectives on the Fourth amendment, 58 Minn.L.Rev. 384(1974)

17. United States v. Wurzbach, 280 U.S. 396, 399 (1930)

18. Edmond, 531 U.S. at 45-46 "Programmatic purposes may be relevant to the validity of Fourth Amendment intrusions undertaken pursuant to a general scheme without individualized suspicion.

19. Harold J. Krent, Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment, 74 TEX. L. REV. 49, 51 (1995).